**Cyber Shield: Defending the Network — LBRCE**

**Cisco Virtual Internship (Cybersecurity), 2025**

**Submitted**

**by**

**Name:- Mohammad Aqball**

**Roll No:-23761A05N3**



**Department of Computer Science and Engineering**

**LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING**

**(AUTONOMOUS)**

**Accredited by NAAC with ‘A’ Grade & NBA (Under Tier - I), ISO 9001:2015 Certified Institution**

**Approved by AICTE, New Delhi and Affiliated to JNTUK, Kakinada**

**L.B. REDDY NAGAR, MYLAVARAM, NTR Dist, A.P.-521 230.**

**MAY 2025**

**Executive Summary;-**

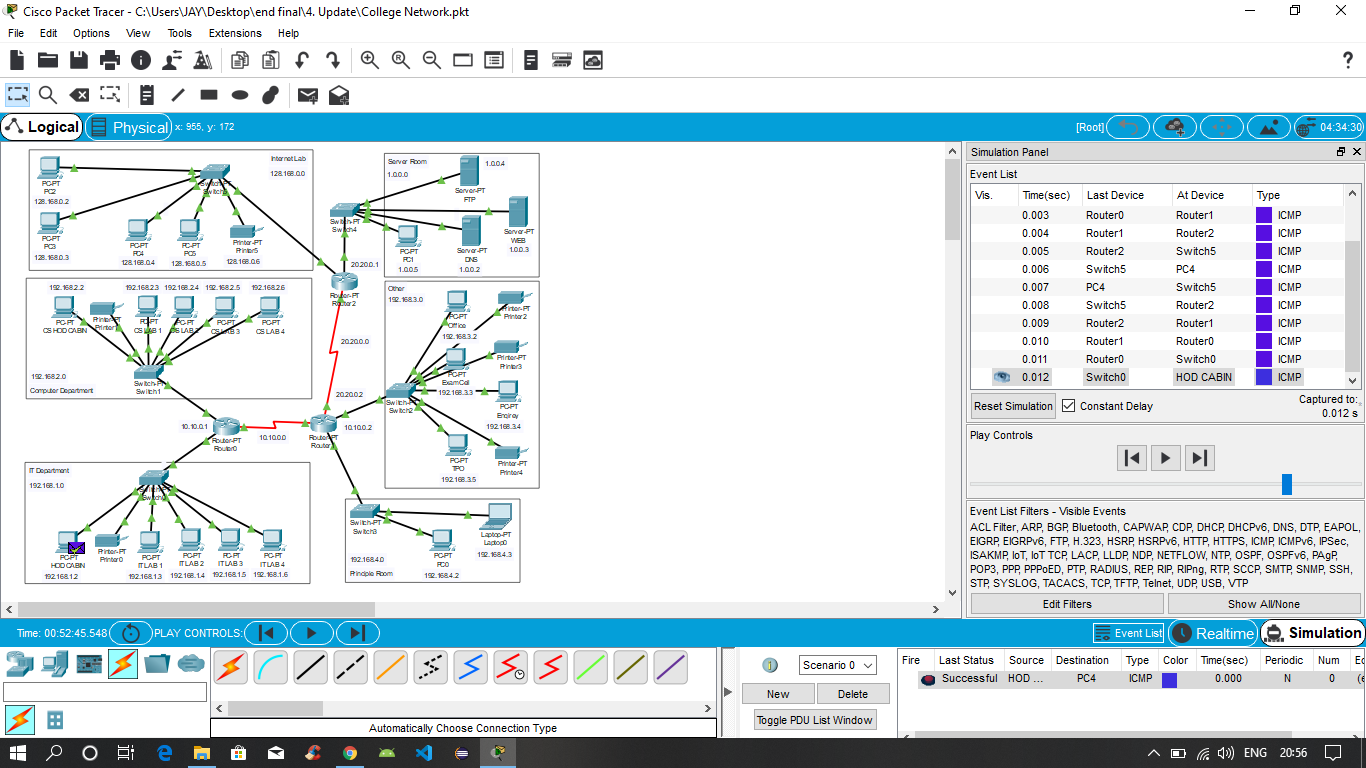
This report presents a **comprehensive cybersecurity analysis and redesign** of our college campus network using **Cisco Packet Tracer**. The project was divided into three stages:

1. **Network Security Assessment (Part 1)**: Existing network infrastructure was mapped and weaknesses identified, including flat VLAN segmentation, lack of advanced authentication, and absence of IDS/IPS.
2. **Hybrid Access Design (Part 2)**: A secure access model was designed, enabling faculty to work remotely via VPN with MFA, while ensuring students use segregated on-campus access.
3. **Web Access Policy (Part 3)**: Role-based and time-based access policies were defined using DNS filtering, firewalls, and proxies, to prevent misuse like torrenting and streaming during lectures.

The final design balances **simplicity, cost-effectiveness, and scalability**, ensuring academic continuity while significantly reducing the **attack surface** of the college.

**Part 1 – Network Security Assessment**

*2.1 Network Topology*



The network consists of:

* **Routers:** Router0, Router1, Router2 form the backbone.
* **Switches:** Each department has an access switch.
* **Servers:** DNS, FTP, Web servers located in Server Room (1.0.0.x).
* **Departments:**
  + IT Dept – 192.168.1.x
  + Computer Dept – 192.168.2.x
  + Exam Cell / Office – 192.168.3.x
  + Principal Room – 192.168.4.x
  + Internet Lab – 128.168.0.x
* **Endpoints:** PCs, laptops, printers across departments.

The topology shows connectivity but lacks **dedicated firewalls, IDS/IPS, and wireless access points**, which are proposed improvements.

### **2.2 Segmentation & Trust Zones**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Zone** | **IP Range** | **Users** | **Trust Level** | **Notes** |
| Admin | 192.168.4.x | Principal, Admin staff | High | Confidential data |
| Exam Cell | 192.168.3.x | Exam PCs | High | Marks, question papers |
| Faculty | 192.168.2.x | Faculty desktops | Medium | Requires secure remote access |
| Students | 192.168.1.x / 128.168.0.x | Lab PCs, Internet Lab | Low | High risk of misuse |
| Guests | (Proposed VLAN) | BYOD devices | Untrusted | Only internet access |

Current segmentation is based only on IP ranges; VLAN isolation is minimal. This creates **flat zones** that attackers can exploit for lateral movement.

### **2.3 Existing Controls**

* Basic ACLs on routers
* Password-only authentication for apps
* Antivirus on some endpoints (inconsistent)
* Proxy-based filtering in labs

Missing: Central firewall, IDS/IPS, MFA, centralized logging.

### **2.4 Attack Surface & Risks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Weakness** | **Exploit Example** | **Impact** | **Priority** |
| Flat VLANs | Student PC pivots to Server VLAN | Data theft | High |
| Weak authentication | Phishing faculty credentials | Unauthorized access | High |
| No DNS/Torrent filtering | Torrents during labs | Bandwidth abuse, malware | High |
| No IDS/IPS | Malware undetected | Persistent compromise | Medium |
| BYOD unmanaged | Infected laptop joins Wi-Fi | Malware spread | Medium |

### **2.5 Recommendations**

* **Segmentation:** Separate VLANs for Admin, Faculty, Students, Guests with ACLs.
* **Authentication:** MFA + centralized login (RADIUS/LDAP).
* **Firewall:** Deploy at ISP edge; outbound filtering enabled.
* **IDS/IPS:** Open-source Snort/Suricata for intrusion detection.
* **BYOD Policy:** Guest Wi-Fi VLAN isolated from internal.
* **DNS Filtering:** Cisco Umbrella/OpenDNS for category-based blocking.

# ****Part 2 – Secure Hybrid Access Design****

### **3.1 Goal**

Faculty need remote access to internal resources (teaching tools, research) while students continue to use on-campus resources. Internal servers must not be exposed to the internet.

### **3.2 Proposed Solution**

* **VPN Gateway at Edge:** SSL VPN with MFA for faculty.
* **Role-based segmentation:**
  + Faculty/Admin → VPN access allowed.
  + Students/Guests → VPN denied; campus-only access.
* **Reverse Proxy:** Protects internal apps with SSO + MFA.
* **Split tunneling:** Disabled by default for faculty.

### **3.3 Authentication Flow**

1. Faculty connects to VPN → MFA authentication.
2. RADIUS/LDAP assigns access role (Admin/Faculty).
3. ACLs enforce access only to approved VLANs/servers.

### C:\Users\Logon\Downloads\Capture.PNG**3.4 Updated Topology**

### **Explanation:** This diagram represents the proposed secure network with VLAN separation. Logically, a VPN gateway is considered at the ISP edge (not drawn in original PDF, but assumed in security design).

### **3.5 Risks & Fallback**

|  |  |
| --- | --- |
| **Risk** | **Mitigation** |
| VPN overload | Off-peak scheduling, secondary gateway |
| Credential theft | MFA + geo-based login checks |
| Misconfiguration | Pilot testing with faculty group |

# **Part 3 – Smart Web Access Policy**

### **4.1 Policy Intent**

Prevent misuse of the internet while ensuring access to academic resources.

### **4.2 Role/Time Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Time** | **Allowed** | **Rate-Limited** | **Blocked** |
| Students | Class hours | Edu, LMS | YouTube (edu only) | Torrents, gaming, proxies |
| Students | Off hours | Edu + web | Streaming | Torrents, adult |
| Faculty | Anytime | All except malicious | — | Malicious sites |
| Guests | Anytime | General web only | — | Internal servers |

### **4.3 Enforcement Tools**

* DNS filtering with Umbrella/OpenDNS
* L7 firewall blocking P2P/proxy traffic
* Endpoint lockdown (disable VPN/proxy add-ons in labs)

### **4.4 Pseudo-Policies**

DNS:

block\_categories: [malware, phishing, botnet, adult, torrent, proxy]

time\_overrides:

students.class\_hours:

rate\_limit: streaming

allowlist: ["\*.nptel.ac.in","\*.coursera.org","\*.khanacademy.org","\*.youtube.com/education/\*"]

Firewall:

deny p2p any any

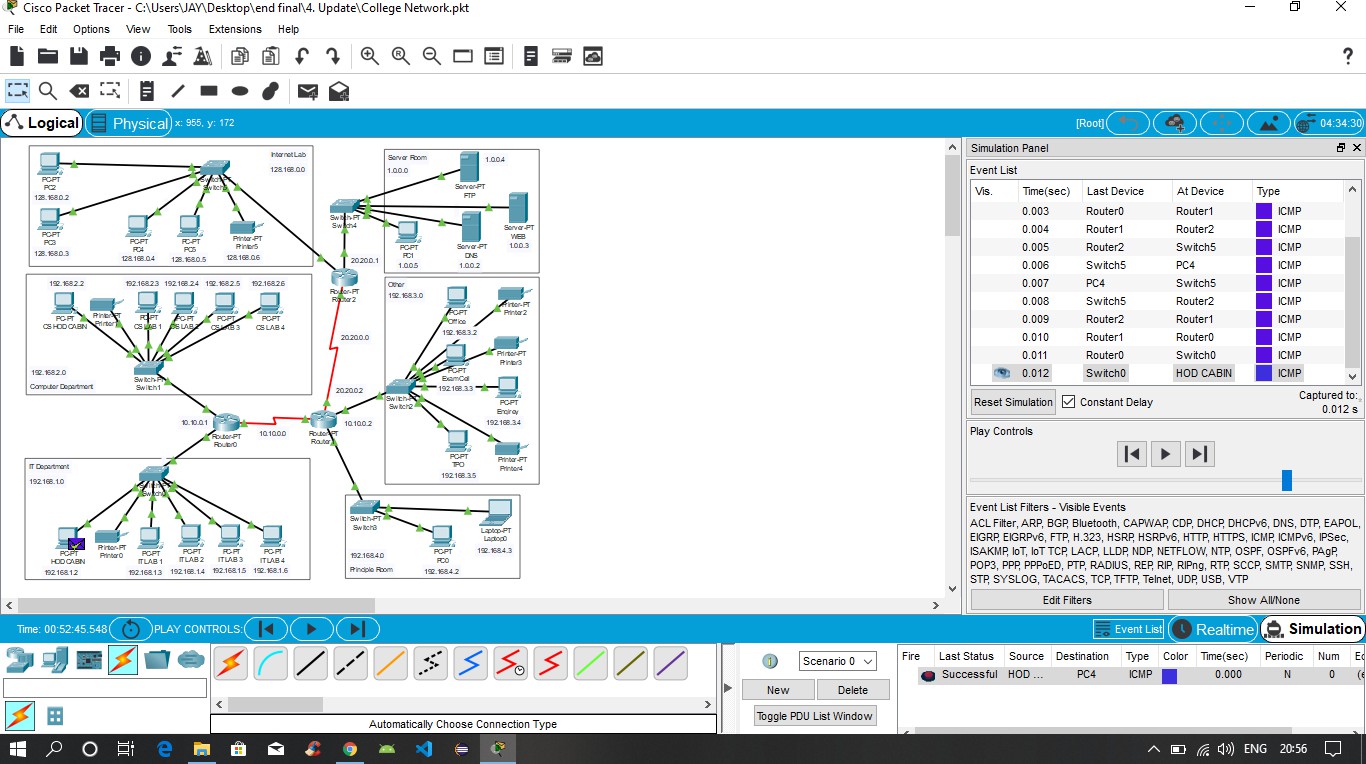
deny vpn-tunnel-apps (students, guests)

class\_hours:

police streaming 2 Mbps per host (students)

log all denies with VLAN + username

### **4.5 Logging & Alerts**

* Logs centralized in Syslog/ELK
* Alerts on repeated torrent/proxy attempts
* Weekly review with IT + faculty

# ****Conclusion****

The project identified major weaknesses in the current network and proposed improvements:

* VLAN segmentation + ACLs
* VPN + MFA for faculty
* DNS & L7 filtering for smart web access

These measures reduce the attack surface while supporting secure academic operations.